Jurnal Info Sains : Informatika dan Sains
Volume 14 , Number 01, 2024, DOI 10.54209/infosains.v14i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

The role of the police in tackling cyber crime on social media

Ahmad Hadi Prayitno[1], Masroor Ridwan[2], Aji Sudarmadji[3]
Faculty of Law, Universitas Islam Sultan Agung Semarang[1,2,3]

Article Info

Keywords:
Police,
Countermeasures,
Crime,
Cyber Crime

ABSTRACT

The development of information and communication technology causes world relations to become borderless and causes significant social, economic, and cultural changes to take place so quickly. On the one hand, technological advances have a positive impact, but also have a negative impact, with the emergence of various types of Cybercrime. Cybercrime or cybercrime is regulated in Law Number 19 of 2016 amending Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), especially in Articles 27 to 30 regarding prohibited acts, then a firm and clear attitude that cybercrime is a criminal act prohibited by law and every perpetrator will be dealt with according to applicable law. The purpose to be achieved from this study is to find out the role of the police in tackling Cybercrime on social media and what obstacles are faced by the police in tackling Cybercrime on social media and how to solve it. Primary Data is obtained through field studies (Fleld Research), while Secondary Data is obtained through literature studies (Library Research) with a series of documentation studies. The analytical method used in this study is empirical juridical. The results of this study show that law enforcement actions and efforts regarding the handling of Cybercrime are in the form of pre-emptive actions, preventive actions and repressive actions. In addition, internal constraints begin with weak government and police supervision, evidence in Cybercrime crimes is easily changed, deleted or hidden by criminals, there are rarely witnesses in Cybercrime cases and unclear jurisdiction determination. In addition, external constraints include law enforcement factors, facilities, community and environment, and cultural factors.

Corresponding Author:
Ahmad Hadi Prayitno
Faculty of Law, Universitas Islam Sultan Agung Semarang
ahprayitno@unissula.ac.id

INTRODUCTION

Advances in the use of information technology, media, and communication have changed both the behavior of society and human civilization globally. The development of information and communication technology has also caused world relations to become borderless and caused significant social, economic, and cultural changes to take place so quickly. Information technology is currently a double-edged sword, because in addition to contributing to the improvement of human welfare, progress, and civilization, it is also an effective means of unlawful acts. Technology makes it easy for people to obtain and convey public information. One of the impacts of globalization is the advancement of developments in the field of technology and information. Developments in the field of technology and information are expected to have a positive impact on human life, which

Jurnal Info Sains : Informatika dan Sains
Volume 14 , Number 01, 2024, DOI 10.54209/infosains.v14i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

will ultimately lead to the creation of improved human welfare. Although in practice the development of technology and information can also have a negative impact, which is called "CyberCrime" or crime through the Internet network. The internet makes crimes that were originally conventional such as the spread of fake news (hoaxes), threats, theft and fraud become more sophisticated through the use of online computer media with a very small risk of being caught by individuals and groups with greater harm to both society and the state in addition to causing new crimes

One of the negative impacts of the internet is cybercrime is a type of crime used by perpetrators related to the use of unlimited information and communication technology in the form of technological engineering. Indonesia is currently one of the countries that has been involved in the use and utilization of information technology, as evidenced by as many as 215 million internet users in 2023. According to the records of the Indonesian Internet Service Providers Association, cyber crimes until mid-2023 will reach 90 million cases. In Indonesia, the city of hackers was first occupied by the city of Semarang, then Yogyakarta.

Cybercrime is a crime committed by a person, group of people and corporations (legal entities) by using or targeting computers or computer systems or computer networks. This crime occurs in cyberspace (virtual) so it has different characteristics from traditional crime. Cyber crime or cybercrime is basically the impact of technological advances that have changed people's habits that were originally conventional into a more modern habit or can be called a high technology society. Cybercrime or cybercrime is regulated in Law Number 19 of 2016 amending Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), especially in Articles 27 to 30 regarding prohibited acts, then a firm and clear attitude that cybercrime is a criminal act prohibited by law and every perpetrator will be dealt with according to applicable law.

Given the rampant cases of cybercrime, there needs to be serious handling by the Police which is one of the law enforcement officials responsible for tackling a crime or crime such as crimes caused by technology. Efforts to combat crime with criminal law are essentially part of law enforcement efforts (especially criminal law enforcement). The politics of criminal law is part of law enforcement policy. The use of legal remedies, including criminal law, as an effort to overcome social problems is included in the field of law enforcement policy. Besides that it aims to achieve the welfare of society in general, the policy of law enforcement is also included in social policy, namely rational efforts to achieve community welfare.

METHODS

This type of research is empirical legal research. Empirical legal research is a type of legal research that serves to look at the law by examining the working of law in society and about the effectiveness of the law that is currently in force. This means that the author immediately conducted data mining on experts at the Semarang Resort Police Investigation and Criminal Unit.

The approach of this study is an empirical juridical approach. The empirical juridical approach is an approach by examining secondary data or data obtained from theoretical foundations such as opinions or writings of experts or legislation first, then continued by

Jurnal Info Sains : Informatika dan Sains
Volume 14 , Number 01, 2024, DOI 10.54209/infosains.v14i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

conducting primary data research in the field such as interviews. An interview is a conversation between two or more people that occurs between the source and the interviewer with the intention of collecting data that is information. The type of interview used by the authors in this study is a structured interview. A structured interview is an interview that uses questions (questionnaires) for respondents. The questions asked in the interview are structured according to what the author wants.

Judging from its nature, this research is included in the category of descriptive research, which is a research in the form of an overview of the implementation of case management mechanisms. The descriptive method is fact-finding of proper interpretation. This descriptive research studies problems in society and certain situations, including the relationship between activities, attitudes, views, and ongoing processes and the influences of a phenomenon in this case is the role of the police in tackling cybercrime.

RESULTS AND DISCUSSION

The State of Indonesia is a State of Law in accordance with the Constitution of the Republic of Indonesia Year 1945 Article 1 paragraph 3 namely "The State of Indonesia is a State of Law" so that all aspects of Indonesian people's lives must be based on law (rechtsstaat). Law Number 2 of 2002 concerning the Indonesian National Police, one of the duties of the police is to investigate and investigate all criminal acts in accordance with the criminal procedure law and laws and regulations. The rise of cyber crime cases, there needs to be serious handling by the Police which is one of the law enforcement officials responsible for tackling a crime or crime such as crimes caused by technology. The duties and functions of the Police are regulated in the Regulation of the Chief of Police Number 6 of 2019 concerning Criminal Investigation stipulating that, Indonesian National Police Investigators of the Republic of Indonesia have duties, functions and authorities in the field of criminal investigation in accordance with the provisions of laws and regulations, which are carried out professionally, transparently and accountably for every criminal case in order to realize the rule of law that reflects legal certainty, a sense of justice and expediency.

Therefore, the police as a law enforcement institution has a very large role in law enforcement, including tackling cyber crime, which is usually handled by cyber police. In the criminal justice system, the police are the first institution to handle all criminal acts by conducting investigations so that it can be said that the success of handling cyber crime depends on the results of police work. Restorative justice is in principle a philosophy (basic guideline), in the peace process outside the court by using mediation or deliberation in achieving justice expected by the parties involved in the criminal law, namely the perpetrator of the criminal act (his family) and the victim of the crime (his family) to find the best solution agreed and agreed by the parties. Everyone hopes that the Police will handle criminal cases so that they can be solved optimally. This is to determine the extent of optimizing the role of the police in tackling cyber crime.

Based on Article 1 point 5 of the Criminal Procedure Code, an investigation is a series of actions / investigations to find and find an event that is suspected to be a criminal offense in order to determine whether or not an investigation can be carried out in the manner regulated in the Law. An investigation was conducted prior to the investigation.

Jurnal Info Sains : Informatika dan Sains
Volume 14 , Number 01, 2024, DOI 10.54209/infosains.v14i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

With the meaning affirmed in the Criminal Procedure Code, the investigation is actually an investigator who seeks or takes his own initiative to find events that are suspected to be criminal acts. Although in carrying out investigation duties, sometimes also receive reports or complaints from the aggrieved party.

Cyber crime is regulated in Law Number 19 of 2016 amending Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law), especially in Articles 27 to 30 regarding prohibited acts, then a firm and clear attitude that cyber crime is a criminal act prohibited by Law and every perpetrator will be dealt with according to the applicable Law. With these regulations, it should be able to reduce or even make cyber crime. But the reality is that lately there are very frequent cyber crimes that harm many people.

The form of solving cyber crime cases according to Law Number 19 of 2016 amends Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law).

1. Any person can file a lawsuit against the party that organizes the electronic system and/or uses information technology that causes losses.
2. The public can file a lawsuit vicariously against parties who organize electronic systems and / or use information that results in harming the community, in accordance with the provisions of laws and regulations.
3. The data lawsuit is carried out in accordance with the provisions of the legal regulations.
4. In addition to the settlement of civil claims as referred to in paragraph (1), the parties may resolve disputes through arbitration, or other alternative dispute resolution institutions, in accordance with laws and regulations.

In tackling the occurrence of cyber crime, the police have made various efforts such as giving appeals to the public through electronic media and social media by disseminating broadcasts in the form of appeals related to cyber crime to be forwarded to the wider community. In addition, information was also carried out to the wider community. In addition, information was also carried out to the public through newspapers and radio media, and when filling in talk shows, the police did not stop giving appeals to the community. The police take action by processing every case of Cyber crime that is handled in accordance with applicable regulations. The police work with existing stakeholders, namely how to catch perpetrators caught committing crimes or through community reports then visit the crime scene (TKP) to make arrests and detentions of suspects in Cyber crime cases, after arrests are made then processed by the police and before being transferred the case file to the prosecutor's office. The role of the police in the context of efforts to overcome cyber crime includes three (3) things, namely pre-emptive actions, preventive actions (prevention), and repressive actions (law enforcement).

Pre-emptive action which is the first step taken by the police to prevent criminal acts. Efforts made in pre-emptive crime reduction are to instill good values / norms so that these norms are internalized in a person. Even if someone wants to commit a crime but there is no intention to do so, there will be no crime. This method of prevention comes from the NKK theory, namely; The intention and opportunity of the crime.

Jurnal Info Sains : Informatika dan Sains
Volume 14 , Number 01, 2024, DOI 10.54209/infosains.v14i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

Preventive efforts are the next step that will be taken from pre-emptive efforts that are still in the level of prevention before the occurrence of crime. This preventive effort is a very easy effort to do because it can be done by anyone for those who can provide knowledge about preventing a crime. In preventive efforts the most important thing is to eliminate an opportunity to commit a crime.

Repressive efforts are the last resort that can be done after pre-emptive and preventive efforts. Repressive effort is a procedural effort in accordance with our legal system, our criminal justice system. This effort is carried out when a criminal act / crime has occurred, this act is referred to as law enforcement by imposing penalties in accordance with predetermined sanctions. Then only certain people can carry out this repressive effort. Namely law enforcement officials, starting from the police.

Police officers in carrying out efforts to combat cyber crime experience several obstacles that hinder efforts to overcome cyber crime.

Internal Constraints

a) Weak supervision of the Government and Police, weak supervision of internet use has great potential to create opportunities for cyber crime (cybercrime) because crimes using technology occur if there is internet access in Indonesia can be said to be adequate both in terms of speed of access and ease of installation of internet access networks. In terms of supervision, the government and police must control and supervise negative internet content traffic that can be accessed in Indonesia. Such as blocking pornographic sites, SARA, violence and websites that are considered to violate moral norms.
b) Evidence in cyber crime is different from other crime evidence where the target or media of cyber crime is data or computer / internet systems that are easily changed, deleted, or hidden by criminals.
c) Victim witnesses in cyber crime cases play a very important role where there are rarely witnesses in cyber crime cases because victim witnesses are outside the region or even abroad which makes it difficult for investigators to examine witnesses and file the results of the investigation. And the last is that the jurisdictional aspect is ignored. Because mapping that concerns cyber health also concerns relations between regions, between regions, and between countries. So that a clear determination of jurisdiction is absolutely necessary.

External factors

There are five external factors that greatly influence law enforcement among several factors interrelated with each other, therefore it is the essence of law enforcement, facilities and infrastructure factors, community factors, and cultural factors.

In law enforcement efforts, there is a need for harmony between various laws and regulations of different degrees. The discrepancy can occur between written and unwritten regulations, between laws of a higher degree and lower regulations, between laws that are specific and general, and between laws that apply before. All of this can affect law enforcement issues because the purpose of establishing a regulation is to provide legal certainty, expediency and justice. For this reason, in order to avoid the occurrence of a

Jurnal Info Sains : Informatika dan Sains
Volume 14 , Number 01, 2024, DOI 10.54209/infosains.v14i01
ESSN 2797-7889 (Online)
https://ejournal.seaninstitute.or.id/index.php/InfoSains

regulation that does not apply effectively in the community, it is necessary to pay attention to the principles and objectives of the law itself.

The police have an important role in efforts to overcome cyber crime, where the ability of the police is needed to uncover cyber crime cases. The existence of a cyber crime unit within the police proves that special investigators are needed who have the ability in the field of information and electronic transactions to handle crimes in cyberspace. Therefore, special education is needed to provide knowledge related to cyber crime to law enforcers who specialize in handling cyber crime problems.

In the function of the law, the mentality or personality of law enforcement officers plays an important role, if the regulations are good, but the quality of officers is not good it will cause problems therefore one of the keys to success in law enforcement is the mentalization or personality of law enforcement. In disclosing cyber crime cases, facilities are needed that are able to support the performance of police officers. The facility is in the form of a computer forensic laboratory that is used to reveal digital data and record and store evidence in the form of softcopy (images, programs, html, sound, and so on). Computer forensics is one branch of forensic science that deals with legal evidence found in computers and digital storage media. In the framework of law implementation, serana and facilities must be adequate because often the law is difficult to enforce because it is hit by factors of inadequate or even non-existent facilities. With the lack of facilities and supporting facilities, law enforcement will be hampered and of course law enforcement officials cannot maximize their actual role.

CONCLUSION

The rule of law is a logical outcome requiring institutions that can supervise law enforcement, one of which is the police. So in order to implement the regulation, it requires the role of the police in the context of efforts to overcome cybercrime including three (3) things, namely pre-emptive actions, preventive actions (prevention), and repressive actions (law enforcement). The obstacles faced by the police in tackling electronic information and transaction (ITE) crimes, internal obstacles begin with weak government and police supervision, evidence in cybercrime crimes is easily changed, deleted, or easily changed, deleted, or hidden by criminals, rarely there are witnesses in cybercrime cases and the determination of jurisdiction is unclear. In addition, external constraints include law enforcement factors, facilities/facility factors, community and environmental factors, and cultural factors (culture).

REFERENCE

Abdul Wahid and Mohammad Labib, 2005, Cyber Crime, PT. Refika Aditama, Jakarta.

Jonaedi Efendi &; Johnny Ibrahim, 2016, Normative and Empirical Legal Research Methods, Jakarta, Kencana.

Marlina., 2009, Juvenile Criminal Justice in Indonesia: Development of Diversion and Restrorative Justice Concepts. Refika Aditama, Jakarta.

Mewengkang, Warong, and Kuntag, 2009, "Juridical Study of Cyber Crime Countermeasures and Law Enforcement." Jakarta.

Moh. Nazir, 2003, Research Methods, Jakarta, Ghalia Indonesia.
Philemon Ginting, 2008, Policy for Combating Information Technology Crime through Criminal Law, Semarang.
Zainuddin Ali, 2015, Legal Research Methods, Jakarta, Sinar Grafika.
JOURNALS AND SCIENTIFIC PAPERS
Anang Sugeng Cahyono, 2016, "The Influence of Social Media on Social Change in Society in Indonesia," Journal Publiciana 9, number. 1.
Indriani Berlian Mewengkang, Robert N. Warong, and Michael Kuntag, 2021, "Juridical Study of Cyber Crime Countermeasures and Law Enforcement," Lex Crimen 10, No. 5.
Lukmanul Hakim, 2018, "Banking Institutions' Accountability for Customer Data Theft," Dialogia Iuridica, Journal of Business and Investment Law 10, Number. 1.
I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, and I Nyoman Gede Sugiartha, 2020, "Law Enforcement Against Hacking as a Form of Cyber Crime," Journal of Legal Construction , Vol. 1, No. 2.
Mewengkang, Warong, and Kuntag, "Juridical Study of Cyber Crime Countermeasures and Law Enforcement."
Petrus Reinhard Golose, 2006, Development of Cyber Crime and Efforts to Overcome It in Indonesia by the National Police, Banking and Central Banking Law Bulitent, Volume 4 Number 2.
Tony Yuri Rahmanto, 2019, "Law Enforcement Against Electronic Transaction-Based Fraud," De Jure Journal of Legal Research, Vol 19, No. 1.
Constitution of the Republic of Indonesia Year 1945
Law Number 2 of 2002 concerning the Indonesian National Police
Law Number 19 of 2016 amends Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law)
Code of Criminal Procedure (KUHP)
Civil Code (KUHPercivil)
Regulation of the Chief of National Police Number 6 of 2019 concerning Criminal Investigation.
Ministry of Communication and Information Technology of the Republic of Indonesia, 2023, "Polri: Indonesia Highest Cyber Crime in the World", https://www.kominfo.go.id/content/detail/13487/polri-indonesia-tertinggi-kedua-kejahatan-siber-di-dunia/0/sorotan_media. Retrieved June 12, 2023.